Claire McCaskill
Missouri State Auditor

December 2006

CONSERVATION

Information Technology Management

Report no. 2006-77

auditor.mo.gov

Claire McCaskill
Missouri State Auditor

YELLOW SHEET

Missing Security Controls Increases Risks of Threats and Vulnerabilities to Information Technology Resources

This audit reviewed the management and control of information technology resources at the Missouri Department of Conservation (MDC). Auditors found MDC management needs to obtain and commit resources to fully document and develop internal control policies and procedures to completely protect the department's information and technology resources from threats and vulnerabilities. Auditors also performed an analysis of fiscal year 2005 department expenditures and found MDC paid $23,232 in potential duplicate payments for products or services.

Risk assessment program is not fully implemented

Identifying and assessing information security risks are essential steps in determining what controls are required and what level of resources should be expended on controls. MDC management had not fully implemented a formal risk assessment process and had no policies for conducting these assessments. A MDC Information Technology Section (ITS) official said informal, undocumented risk assessments have been performed. According to another ITS official, ITS does not have the resources available to dedicate to performing and documenting a formal risk assessment. (See page 5)

Business continuity and disaster recovery plans not approved and implemented

MDC personnel have documented a business continuity plan and a disaster recovery plan. However, neither of these plans has been approved by management. Since the plans have not been approved, an ITS official said neither plan has been implemented or tested. Without implementing and testing these two plans, management cannot ensure the adequacy of the plans. Management does not have assurance that critical business operations could be carried out or computer operations promptly restored in the event of a significant disruption to normal system operations. (See page 5)

Security management program is not fully implemented

MDC management has developed and documented policies for specific security controls, including password standards and establishing user access. However, MDC management had not completed the process of establishing and documenting policies and procedures for all key security controls. Accepted standards state policies are necessary to set organizational strategic directions for security and assign resources for the implementation of security. (See page 6)

Payment procedures not always followed

Our analysis of fiscal year 2005 department expenditures found MDC overpaid vendors up to $23,232 for the same products or services because of internal control weaknesses. Duplicate payments can occur for a variety of reasons, including data input errors, inconsistencies in the vendor file, and payments from non-original invoices such as statements and faxes. As a result of our findings and questions, MDC management began an internal audit of duplicate payments and related internal controls. (See page 14)

All reports are available on our website: www.auditor.mo.gov

Contents

Abbreviations

GAO	Government Accountability Office
ITS	Information Technology Section
MDC	Missouri Department of Conservation

CLAIRE McCASKILL
Missouri State Auditor

Honorable Matt Blunt, Governor
and
Conservation Commission
and
John Hoskins, Director
Department of Conservation
Jefferson City, MO 65102

The Missouri Department of Conservation (MDC) is responsible for protecting and managing the fish, forest and wildlife resources of the state. The Information Technology Section is responsible for providing technical assistance to support MDC technology resources. Our audit objectives included determining whether MDC management has established effective internal controls over information systems, information technology resources, and over the processing of department expenditure and payment transactions.

We found MDC had not taken some of the measures necessary to maintain effective internal controls to protect the information and technology resources supporting the mission and operations of the department. MDC had not fully implemented risk assessment and security management programs to identify and manage security controls required to protect the department's systems and resources from potential threats and vulnerabilities. We also found MDC had not finalized, approved, or implemented contingency plans necessary to sustain and recover critical technology services following an emergency. We found instances where important security policies had not been developed and instances where procedures were in place but the corresponding policies had not been documented. In addition, we found weaknesses in internal control procedures over the processing of department expenditure transactions which caused the erroneous processing of duplicate payments.

We conducted our audit in accordance with applicable standards contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, and included such procedures as we considered necessary in the circumstances. This report was prepared under the direction of John Blattel. Key contributors to this report were Jeff Thelen, Lori Melton, and Frank Verslues.

Claire McCaskill
State Auditor

Introduction

The Missouri Department of Conservation (MDC) is responsible for protecting and managing the fish, forest and wildlife resources of the state; serving the public and facilitating participation in resource management activities; and providing opportunity for all citizens to use, enjoy and learn about fish, forest and wildlife resources, according to the department's mission statement. The MDC Information Technology Section (ITS) supports the department's mission through technological solutions and electronic communications.

ITS provides support and management of information technology resources for MDC. Information, some of which is sensitive, maintained in MDC systems includes:

- Hunting and fishing permits and licenses
- Wildlife protection investigations and arrests
- Human resource and department expenditure records
- Geographic information system data

Disclosure of specific sensitive data maintained in MDC systems could compromise department enforcement activities. In addition, unauthorized access to personal information could increase the risk of identity theft.

Effective July 1, 2005, information technology personnel and resources from most executive branch agencies[1] were consolidated and placed under the direction of the state Chief Information Officer in the Office of Administration, Information Technology Services Division. Information technology personnel and resources from MDC were not included in this consolidation. However, the ITS Chief Information Officer stated MDC attempts to follow the guidelines, including the Missouri Adaptive Enterprise Architecture,[2] set by the Information Technology Services Division.

Scope and Methodology

To determine whether MDC management had established effective internal controls to manage and protect information technology resources we requested and reviewed available policies and procedures and other

[1] Entities such as the Department of Conservation, governed by commissions, are not included in the information technology consolidation. In addition, entities not under the Governor, such as elected officials and the state courts system, are not included in the consolidation.

[2] The Enterprise Architecture is made up of several information technology domains, including a domain dedicated to security. The security domain is not fully developed, but it defines the security management principles which are needed to help ensure the appropriate level of protection for the state's information and technology assets.

documents and interviewed MDC and ITS personnel. We also interviewed MDC and ITS personnel to gain an understanding of the undocumented and informal procedures and controls in place.

To obtain an understanding of the general operations of MDC, we obtained and analyzed MDC expenditure data for fiscal year 2005 from the statewide accounting system. During our analysis, we identified transactions that were potential duplicate payments for the same products or services. To verify the accuracy of the expenditure data, we obtained the source documents for these potential duplicate payments from the Office of Administration. We reviewed these source documents to verify the payment amount agreed to the expenditure data from the statewide accounting system. We provided the MDC internal auditor and a payment staff employee a list of the potential duplicate payments and discussed the payments with them.

We based our evaluation on accepted state, federal, national and international standards and best practices related to information technology security controls from the following sources:

- Missouri Adaptive Enterprise Architecture
- National Institute of Standards and Technology
- U.S. Government Accountability Office (GAO)
- IT Governance Institute Control Objectives for Information and related Technology (COBIT)

We requested comments on a draft of our report from the Director of the Department of Conservation. We conducted our work between June and October 2006.

Missing Security Controls Leaves Technology Resources Susceptible to Threats and Vulnerabilities

MDC information technology resources are susceptible to threats and vulnerabilities including unauthorized use and disclosure of data and insufficient protection of technology assets. This situation has occurred because MDC management had not (1) performed a formal risk assessment to identify possible threats and the likelihood of occurrence, (2) approved and implemented business continuity and disaster recovery plans to ensure the availability of technology resources, and (3) fully implemented a security management program. In addition, key policies and procedures for internal controls, including security, had not been documented or had not been developed. Collectively, these weaknesses impair MDC's ability to ensure information technology resources are properly protected and the risk of threats and vulnerabilities are reduced to an acceptable level.

Risk Assessment Program Is Not Fully Implemented

Identifying and assessing information security risks are essential steps in determining what controls are required and what level of resources should be expended on controls. Moreover, by increasing awareness of risks, these assessments generate support for the adopted policies and controls, which helps ensure policies and controls operate as intended, according to GAO. A risk assessment helps identify potential threats and vulnerabilities or weaknesses that could be exploited and to ensure appropriate controls are implemented to mitigate these vulnerabilities.

MDC management had not fully implemented a formal risk assessment process and had no policies for conducting these assessments. An ITS official said informal, undocumented risk assessments have been performed. According to another ITS official, ITS does not have the resources available to dedicate to performing and documenting a formal risk assessment. Since risks and threats change over time and employees leave, the results of risk assessments should be documented to ensure an appropriate action plan is developed to limit vulnerabilities and to reduce risk to an acceptable level.

Business Continuity and Disaster Recovery Plans Not Approved and Implemented

Contingency planning is designed to mitigate the risk of system and service unavailability by focusing effective and efficient recovery solutions. Ultimately, an organization would use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization’s information systems, business processes, and the facility, according to accepted standards.

MDC personnel have documented a business continuity plan and a disaster recovery plan. However, neither of these plans has been approved by management. A MDC official explained the business continuity plan had been developed by a contractor. A draft of the plan had been received in July 2006, and is still under review by MDC personnel. The plan will be presented to management for approval after the review process has been

completed. This official added the disaster recovery plan will be presented for approval at the same time as the business continuity plan. Since the plans have not been approved, an ITS official said neither plan has been implemented or tested. Without implementing and testing these two plans, management cannot ensure the adequacy of the plans. Management does not have assurance that critical business operations could be carried out or computer operations promptly restored in the event of a significant disruption to normal system operations.

Security Management Program Is Not Fully Implemented

A security management program provides a framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of an agency's security controls. A security management program is the foundation of an agency's security control structure and a reflection of management's commitment to addressing security risks. According to GAO, implementing a security program is essential to ensuring controls over information and information systems work effectively on a continuing basis.

MDC management has not fully established a security management program on which department-wide security policies, standards, and procedures can be formulated, implemented, or monitored. ITS officials said MDC follows the Missouri Adaptive Enterprise Architecture security domain as its architecture framework when it is feasible for MDC to do so. The security domain is not fully developed, but it defines the security management principles needed to ensure the appropriate level of protection for the state's information and technology assets. When completed, the security domain architecture will provide a security plan template for agencies to use as guidance when developing agency plans; the architecture will not provide an actual plan for agencies to implement.

Although the security domain architecture is not fully developed, other standards are available for security management planning. Accepted standards state policies are necessary to set organizational strategic directions for security and assign resources for the implementation of security. According to GAO, a critical element of an effective security management program is developing and implementing policies and procedures to govern security over an agency's information technology environment.

MDC management developed and documented policies for specific security controls, including password standards and establishing user access. However, MDC management had not completed the process of establishing and documenting policies and procedures for all key security controls.

MDC needs to develop policies for critical security controls

MDC management had not established or documented policies or procedures for the following critical security controls:

- System and data ownership
- System and data classification
- Security activity logging and review
- Supervisory review of user access rights
- Security awareness training

System and data owners are not designated

The Missouri Adaptive Enterprise Architecture states information owners are necessary to administer information security. It is important to document the ownership of data and information systems because owners make decisions about classifying and protecting information and systems, according to accepted standards.

MDC management does not have documented policies identifying the data and system resource owners responsible for making decisions regarding data classification and system access. An ITS official said a policy is under development, but has not been completed as of October 2006. Without having documented policies and procedures establishing data and information ownership responsibilities, the MDC is at risk that data and information assets will not be properly protected against unauthorized access.

Systems and data are not classified according to sensitivity and criticality

MDC management does not have assurance that systems and data receive an appropriate level of protection. MDC had not established a department-wide framework for systems and data classification, according to an ITS official. Such a framework examines the sensitivity of both the data to be processed and the system itself to identify when to classify information as confidential, public, or other established levels, according to accepted standards.

A general classification framework is established to define an appropriate set of protection levels and the placement of data in information classes, according to accepted standards. Sensitivity is generally classified in terms of confidentiality, integrity, and availability. Factors such as the importance of the system to the organization's mission and the consequences of unauthorized use of the system or data need to be examined when assessing sensitivity. An ITS official said a classification framework had not been developed because the department was waiting for policy from the Office of Administration Information Technology Services Division in this area. The Information Technology Services Division has issued a draft standard on data classification, but the standard has not been finalized as of October 2006.

Policies needed to log, report and review security activity

MDC management had not taken sufficient steps to ensure system security controls have functioned properly. Policies and procedures for logging appropriate security-related events and monitoring specific access are necessary when developing effective security programs. Accepted standards state a logging and monitoring function enables the early detection of unusual or abnormal security activity[3] that may need to be addressed to ensure the approved security level is maintained.

System security logging is available on MDC systems; however, ITS officials have not activated this function. Officials stated resources are not currently available to adequately review and analyze these logs if they were activated.

Determining what, when, and by whom specific actions were taken on a system is crucial to establishing individual accountability, investigating security violations, and monitoring compliance with security policies, according to GAO.

Supervisory review of user access rights is needed

MDC management does not have a process in place for supervisors to perform periodic reviews of user access to data and other information resources to determine whether the access rights remain commensurate with job responsibilities. According to the Missouri Adaptive Enterprise Architecture, agencies must periodically review user accounts. At a minimum, this review should include the following (1) levels of authorized access for each user, (2) identification of inactive, idle or orphaned accounts, and (3) whether required training or certification has been completed. Accepted standards also support regular management review of all accounts and related privileges. Without a supervisory review of user access rights, there is an increased risk that unauthorized alterations of these rights will go undetected or that access rights are not aligned with current job duties.

Employees do not receive ongoing security awareness training

Training is an essential component of a security management program. Computer intrusions and security breakdowns often occur because computer users fail to take appropriate security measures. For this reason, it is vital employees using computer resources be aware of the importance and sensitivity of information handled, as well as business and legal rationale for maintaining its confidentiality, integrity, and availability, according to GAO.

[3] Security activity includes users attempting to access data they are not authorized to access, performing a task they are not authorized to perform, or accessing data they are authorized to access that is of a sensitive nature.

An ITS official said personnel had not been trained on an ongoing basis regarding computer security and their roles in ensuring appropriate use of department resources. New employees receive security training as part of orientation, but employees do not receive any other security awareness training. According to accepted standards, employees play a crucial role in helping ensure the security of computer systems and information technology resources. Accepted standards also state ongoing training programs are necessary to maintain employees' security awareness to the level required to perform effectively.

Documented policies are needed for established security procedures

MDC management established, but had not documented, policies and procedures for the following security controls:

- Management of privileged accounts
- Segregation of duties
- Network operations
- Security incident handling
- Physical security

ITS officials explained policies and procedures had not been formally documented for these areas because of a lack of dedicated resources.

Policies needed for managing privileged accounts

MDC management had not documented policies for the administration of privileged user accounts. According to accepted standards, user account management procedures should be established for all user accounts, including system administrators. MDC has documented procedures for granting and removing access to system accounts, but these procedures do not include access to and administration of privileged accounts. ITS officials explained the number of privileged accounts is limited and management reviews their access annually. Without documented policies for the administration of privileged user accounts, management cannot ensure access to those accounts has been appropriately granted to only authorized individuals.

Policies needed to ensure segregation of duties

Inadequately segregated duties increase the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, or computer resources damaged or destroyed, according to GAO. Although duties have been informally segregated, there has not been a formal effort to identify incompatible duties or to create a policy requiring segregation of duties among information technology staff, according to ITS officials. In addition, MDC had no policies in place to review logical access to ensure adequate segregation of duties. Accepted standards state policies should be established to require a division of roles and responsibilities that should exclude the possibility for a single individual to subvert a critical process.

Network operation policies not documented

According to accepted standards, network operating policies and standards for the general control of the organization's network should be established, documented and maintained on a current basis. ITS officials have established network operating controls related to system performance and usage monitoring, software copyright, network start-up, and staff responsibilities. While ITS officials have established operating controls, the network operation policies and procedures are not documented. Without documented policies and standards for general control of the network, there is an increased risk that network controls will erode over time and not remain appropriate.

Security incident handling procedures not documented

MDC management established, but had not documented, computer security incident handling responsibilities and duties. Computer security incident handling is the process of detecting and analyzing computer security incidents[4] and limiting each incident's effect, according to accepted standards. ITS officials explained MDC monitors for incidents and coordinates with the Office of Administration when necessary.

An incident response policy should be created as a foundation for incident response procedures. Without formally documented procedures, no guidelines exist to ensure the priorities of the organization are reflected in response operations to consistently handle security incidents, according to accepted standards. As a result, incidents may not be handled in the most optimal manner, leaving the network or other systems vulnerable.

Physical security policy not documented

MDC management does not have documentation to ensure adequate physical security is in place to restrict access to computer resources to only appropriate individuals. Management also cannot ensure employees are aware of physical security procedures and what is expected of them in relation to security. MDC management established procedures for physical security, but had not documented the policies or procedures. According to accepted standards, a formal, documented, physical and environmental protection policy addressing the purpose, scope, roles, responsibilities, and compliance should be developed. In addition, an organization should develop, disseminate, and periodically review formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

[4] The Office of Administration Information Technology Services Division defines a security incident as an adverse event, or threat of an adverse event, in a computer system and/or network.

As part of the physical security policy, accepted standards state access to the premises should be logged and monitored. Access to the MDC computer facility is controlled and monitored through the use of key cards. MDC's informal policy also requires visitors to be escorted while in the facility. However, a log of visitors to the computer facility is not maintained. Without a log of the visitors to the facility, management cannot adequately track who had access to the facility.

Conclusions

MDC management had not taken some necessary steps to fully implement effective internal controls to prevent the unauthorized use and disclosure of data and to adequately protect information technology resources. MDC management does not have assurance appropriate controls are in place to reduce risks of threats and vulnerabilities to an acceptable level since a formal risk assessment has not been performed. The recovery of services, systems and technology resources may be delayed following a disruption in operations or a disaster since MDC management had not approved and implemented business continuity and disaster recovery plans. MDC's internal control environment is missing important security components because management had not fully implemented a security management program. Important security controls have not been established or have been developed but lack documented policies and procedures to provide consistent guidance. Faced with the challenge of protecting systems and resources from continuing threats, vulnerabilities, and data breaches, MDC management should support establishing and documenting internal controls and security measures as a business necessity rather than just another management responsibility.

Recommendations

We recommend the Director of the Department of Conservation:

2.1 Implement and document a risk management and assessment framework, which includes policies, standards, and procedures for performing periodic risk assessments so management can better protect the department's resources and its ability to perform the department's missions.

2.2 Complete the process of documenting and approving the business continuity plan. The plan should then be tested and implemented to ensure business operations can continue in the event of a disruption to normal operations.

2.3 Complete the process of documenting and approving the disaster recovery plan. The plan should then be tested and implemented to ensure data and systems on MDC technology resources can be promptly restored in the event of a disaster or other disruption.

2.4 Design, develop, and approve a security management program that provides a framework upon which department-wide security policies, standards, and procedures are formulated, implemented, and monitored. At a minimum, management should implement security controls and document policies and procedures by taking the following actions:

- Ensure all information assets (data and systems) have an appointed owner who makes decisions about data classification and access rights.
- Establish a system and data classification framework to ensure all systems and data are classified in terms of criticality and sensitivity.
- Develop policies and procedures to log, monitor, report, and review appropriate security activity and security violations.
- Periodically review user access to data and other information resources to ensure access rights are commensurate with user's job duties and responsibilities.
- Establish an ongoing security awareness program to communicate the security policy and to assure a complete understanding of the importance of security by all personnel.
- Document policies for the administration of privileged user accounts.
- Document policies to ensure adequate segregation of incompatible duties.
- Document the operating policies and standards for the general control of the network.
- Develop policies and document the current procedures for incident handling and response to ensure the security priorities of MDC are reflected in the response procedures, and that a consistent approach is used in handling security incidents.
- Document policies for physical security, including policies related to visitor escort. In addition, maintain a log of visitors to the computer facility.

Agency Comments

As the report indicates, there are security controls in place for the protection of our IT resources and there have been no documented system breaches to date. The Department's Information Technology Section has taken numerous steps to establish and maintain these controls and we understand the need to have these practices documented, as recommended. We also understand the importance of establishing risk and security management programs; informal, undocumented risk assessments are performed on a periodic basis. Recognizing the importance of IT, the Department has a committee that includes top management from all divisions that specifically reviews and addresses the IT requirements for all divisions and allocation of limited IT Section staffing and funding. Your report will be submitted to this committee for review and consideration. We will continue to do all possible to ensure the security and integrity of our IT resources with the resources available.

Internal Controls Need to be Improved to Prevent Duplicate Payments for Products and Services

MDC erroneously paid up to $23,232 in duplicate payments for the same products or services. MDC made the duplicate payments, in part, because department procedures had not been followed. In addition, the duplicate payments had not been discovered because MDC did not have procedures to monitor for duplicate payments in place.

Payment Procedures Not Always Followed

During our analysis of fiscal year 2005 department expenditures, we identified 21 transactions totaling $23,232 in potential duplicate payments for the same products or services. We found the potential duplicate payments by searching for transactions having the same payment amount and invoice number but different vendor names. We provided the potential duplicate payments along with the corresponding transactions to MDC management. As a result of our findings and questions, MDC management began conducting an internal audit of duplicate payments to identify (1) how many of the potential duplicate transactions we identified are in fact duplicate payments, (2) if other duplicate payments occurred in subsequent years, (3) why or how these duplicate payments had been made, and (4) how these problems could be avoided in the future. Although the internal audit had not been completed at the end of our fieldwork, the MDC internal auditor said at least some of the transactions we identified were duplicate payments and the department had initiated procedures to request refunds from the applicable vendors.

Duplicate payments can occur for a variety of reasons, including data input errors, inconsistencies in the vendor file, and payments from non-original invoices such as statements and faxes. MDC management has documented purchasing and invoice processing procedures that give guidance for payments. The procedures specify, among other details, that payment can only be made from the vendor's invoice or from statements supported by invoices but not from other documents such as packing slips or order acknowledgements. However, MDC personnel did not always follow these procedures when making payments. For example, the source document for one of the potential duplicate payments we found had "Duplicate" printed at the top. We also found other cases where payment for the same products had been made from both invoices and other documents.

A payment staff employee said MDC relies on a function within the statewide accounting system to check for duplicate payments. This edit does not allow an invoice number to be entered more than once for a vendor number. The edit is specific to the entire vendor number and does not evaluate invoices for any related vendors, such as those with the same tax identification number having different locations or addresses. Of the 13 pairs of vendors we reviewed for potential duplicate payments, 8 represented related vendors. Since the statewide accounting system was not

designed to identify duplicate payments to related vendors, MDC must do additional work to ensure these duplicate payments are not made.

Conclusions

MDC management had not minimized the risk of making duplicate payments for the same products or services. Management had not ensured personnel follow payment procedures and had not established procedures to monitor for duplicate payments. Our analysis of fiscal year 2005 department expenditures found MDC overpaid vendors up to $23,232 because of internal control weaknesses. As a result of our identification of these potential duplicate payments, MDC initiated an internal audit to identify the extent of the problem and to determine which duplicate payments need to be recovered.

Recommendations

We recommend the Director of the Department of Conservation:

3.1 Ensure duplicate payments are recovered from the applicable vendors.

3.2 Decrease the chance for duplicate payments in the future by ensuring established procedures are followed and establishing additional procedures to monitor for duplicate payments.

Agency Comments

Our Internal Auditor and Financial Services staff are in the process of reviewing these potential duplicate payments. Steps have been taken to obtain refunds where applicable and additional procedures to prevent future duplicate payments will be considered.